SUBJECT: Application and Computer System(s) Requirements for Complying with 21 CFR Part 11 under the caBIG™ Program	SOP No.: CV-001
	Version No.: 2.0
	Effective Date: 12/11/2006
	Page 1 of 7 Pages

Standard Operating Procedure –

Application and Computer System(s) Requirements for Complying with 21 CFR Part 11 under the caBIG™ Program

This cover sheet controls the layout and components of the entire document.

Issued Date: October 30, 2006

Effective Date: December 11, 2006

Department Approval:

Peter Covitz

Chief Operating Officer, NCICB

QA Approval:

George Komatsoulis

Director of Quality Assurance

Note: This document will be issued for training on the Issue Date. The document will become available for use to trained personnel on the Effective Date. Before using this document, make sure it is the latest revision. Access the caBIG™ website to verify the current revision.

Revision History

Revision	Date	Author	Change Reference	Reason for Change
1.0	09/19/2005	SOP Working Group	N/A	Initial release.
2.0	10/30/2006	BP SIG/SOP WG	All pages	Annual update.

1. Purpose

This Standard Operating Procedure (SOP) describes the process for providing a consistent approach to determine the applicability of 21 CFR Part 11 to computer systems and applications developed, implemented and managed for the conduct of clinical trials under the caBIG™ Program at the NCI. This SOP will also identify the requirements to assure the security, authenticity and trustworthiness of electronic records and electronic signatures (ERES) as defined by Title 21 of the Code of Federal Regulation, Part 11 (21 CFR Part 11), entitled "*Electronic Records; Electronic Signatures*".

2. Scope

2.1 This SOP applies to all computerized systems and/or applications that are used in the conduct and support of clinical trials (subject to regulatory authority and inspection) and that store electronic records on durable medium (e.g. disk, diskette, tape, CD-ROM).

2.2 This SOP does not apply to paper records transmitted by electronic means such as fax, or to word-processed documents that are subsequently printed, authorized and maintained as paper records.

2.3 All caBIG™ sites that develop, configure, maintain, install or use computer systems or applications that create, modify, delete, copy and/or delete electronic records or electronic signatures are responsible for complying with this SOP.

3. Requirements

3.1 **Electronic Records**

3.1.1 An electronic record in the context of this SOP is any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved, copied, deleted or distributed by a computer system and/or application in support of cancer research conducted or sponsored by the NCI under the caBIG™ Program.

3.1.2 Personnel who control systems that create, modify, maintain, archive, copy, delete, retrieve or distribute electronic records must implement and maintain procedures and controls that are designed to protect the authenticity and integrity of the electronic record and electronic signature, and when appropriate, the confidentiality of electronic records from the point of their creation to the point of their deletion.

3.1.3 Electronic records subject to signature must be signed either electronically or, where acceptable, to local regulations, by handwritten signatures. Handwritten signatures must be unambiguously linked to their associated electronic record. Where handwritten signatures are applied to printed out electronic records, both electronic records and signed paper must be maintained.

3.1.4 The computer system or application must be able to restrict access to authorized users and employ computer-generated audit trails to track actions (who and when) to create, modify, or

delete electronic records. Audit trail documentation of electronic records must be automatically date and time stamped by the system.

3.1.5 Electronic records together with any required audit trails and any associated electronic signatures must be maintained and retrievable in a readable form throughout the record's retention period.

3.1.6 Procedures must be established to meet requests from regulatory authorities for access to or copies of electronic records. Where copies of electronic records are provided to regulatory authorities, exact duplicate copies must be made and retained for future reference.

3.1.7 Persons responsible for developing, maintaining or using electronic records must be trained and have the proper education or experience to perform the assigned tasks.

3.2 **Electronic Signatures**

3.2.1 An electronic signature is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. In the context of this SOP, an electronic signature is any legally admissible electronic signing applied by an individual to an electronic record that is used for regulatory submission or is required by local laws and relevant regulations.

3.2.2 Cancer research sites conducting clinical research trials under the caBIG™ Program must assure that individuals are trained and fully grasp their accountability and responsibility for actions initiated under their electronic signatures.

3.2.3 Application of electronic signatures must include the date/time of signature and a unique identifier of the signer.

3.2.4 Electronic signatures must be unique to an individual and not be reused or reassigned to another individual. Persons using electronic signatures (the NCICB Division) must provide documentation (submitted in paper form and signed with a traditional handwritten signature to: Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857) certifying that the electronic signature in the system or application is intended to be the legally binding equivalent of traditional handwritten signatures.

3.2.5 Electronic signatures must be unambiguously linked to their corresponding electronic records.

3.2.6 Procedures and controls must be maintained to ensure that electronic signatures cannot be falsified by ordinary means.

3.2.7 Any disclosure of confidential electronic signature components between staff and the use of another persons' electronic signature is unacceptable and considered falsification of records.

3.2.8 Ability to apply electronic signatures must be withdrawn for individuals whose role no longer includes a signing function (*e.g.* new role, or no longer employed by the cancer research site).

3.2.9 Persons responsible for developing, maintaining or using electronic signatures will be trained and have the proper education and experience to perform the assigned task.

3.3 **Validation**

3.3.1 Computerized systems or applications supporting the regulated use of electronic records and/or electronic signatures (ERES) must be validated (tested) in accordance with requirements identified in 21 CFR Part 11. Testing must cover both technical and procedural controls of systems or applications covered by the regulation.

3.4 **Regulatory Impact Determination Questionnaire**

3.4.1 A computerized system or application should be evaluated to determine if the computer system or application has a regulatory impact (is subject to inspection) and is also subject to 21 CFR Part 11.

3.4.2 A positive output from the regulatory impact assessment tool will be used to conduct a detailed ERES risk assessment of the computer system and/or application.

3.5 Detailed ERES Risk Assessment

3.5.1 A detailed ERES risk assessment should occur to determine whether the computerized system or application meets all of the policy, procedural and technical requirements of 21 CFR Part 11. The results of the detailed assessment will help identify any specific procedural and/or technical enhancement for establishing compliance with 21 CFR Part 11. This detailed assessment will also aid in identification of any interim controls or procedures that may be required for compliance, in ranking the criticality of the compliance gap(s), and listing the actions (temporary or permanent) needed to remediate and/or reduce the risk.

3.6 Risk Assessment and Decision Analysis

3.6.1 A decision analysis tool should be used to quantify (rank) risks in a standard and consistent manner for all computer systems and/or applications under the caBIG™ Program that are subject to regulatory inspection and covered under 21 CFR Part 11 regulation.

4. References/Regulations/Guidelines

Section	SOP Number	Title
4.1	N/A	CDISC Glossary
4.2	N/A	Title 21 CFR Part 11

5. Roles & Responsibilities

Role	Responsibility
System/Application Owner	• Provide funding and resources necessary for ERES systems and personnel to comply with the requirements outlined in this SOP. • Ensure that the system is designed to comply with 21 CRF Part 11 requirements and that tests are conducted to validate compliance. • Produce the necessary documentation to demonstrate that electronic records/electronic signatures are created and maintained in compliance with this SOP.
NCICB Information System Security Officer (Application ISSO)	• Review the ERES Risk Assessment to determine acceptable implementation of information security requirements. • Define acceptable methods for implementing electronic signatures. • Establish procedures for issuing, recalling and revising system passwords. • Conduct security reviews to ensure that the system complies with NCI and regulatory security requirements/guidelines.
Local QA	• Review ERES systems and documentation for compliance with this SOP prior to deployment. Sign-off that the system deployed is compliant with this SOP and thereby, compliant with 21CFR Part 11. • Conduct random audits of electronic records and audit trails to determine if a data breach has occurred in the system.
Systems Administrator	• Ensure electronic signature associated with electronic records belongs to the individual submitting the records. • Perform audit checks to verify that record contents have not been falsified or altered by an unauthorized user. • Perform audit checks to ensure access to electronic records is protected and limited to authorized users. • Perform routine backup and maintenance on electronic records. • Employ the use of passwords to detect and report unauthorized attempts to access information stored in electronic records. • Manage user access to system information; performs initial and periodic testing of user identification devices (e.g., tokens or cards) to ensure that they function properly and have not been altered in an unauthorized manner.

6. Attachments

This SOP will be used in conjunction with the following attachments. These attachments must be used by all research sites conducting clinical trials under the caBIG™ Program and can be customized by individual research sites to accommodate format and content in accordance with local guidelines and/or requirements.

TITLE	DESCRIPTION
1) Procedure Description for Complying with Title 21 CFR Part 11	This document provides step-by-step guidance for complying with Title 21 CFR Part 11.
2) Regulatory Impact Questionnaire	A questionnaire to determine if computerized systems or applications have regulatory impact and are covered by Title 21 CFR Part 11
3) Detailed ERES and Risk Assessment Tool	A tool to aid in conducting a high-level risk assessment of electronic records and electronic signature (ERES) systems and/or application requirements under Title 21 CFR Part 11, identifying and ranking risks associated with non-compliance and identifying remediation activities to reduce outages
4) Process Flow for Complying with Title 21 CFR Part 11	This process flow provides a visual guide outlining the individual steps that need to be followed to comply with Title 21 CFR Part 11.